Multicast in een Campus Network: CGMP- en IGMP-signalering

Inhoud

Inleiding

Het doel van Cisco Group Management Protocol (CGMP) en Internet Group Management Protocol (IGMP) sneoping is om multicast verkeer in een geschakeld netwerk te beperken.

Standaard zal een LAN-switch het multicast verkeer binnen het uitgezonden domein overspoelen en kan deze een hoop bandbreedte consumeren als veel multicast servers stromen naar het segment verzenden.

Voordat u begint

Conventies

Zie de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Voorwaarden

Er zijn geen specifieke voorwaarden van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Achtergrondinformatie

Multicastverkeer wordt overstroomd omdat een switch gewoonlijk de adressen van MAC leert door in het bronadresveld van alle frames te kijken die het ontvangt. Een multicast MAC-adres wordt nooit gebruikt als bronadres voor een pakket. Zulke adressen verschijnen niet in de MAC adrestabel, en de switch heeft geen methode om ze te leren.

De eerste oplossing voor deze kwestie is om statische MAC adressen voor elke groep en elke client te vormen. Deze oplossing werkt echter goed, ze is niet schaalbaar en ook niet dynamisch. U gebruikt deze oplossing op een Catalyst 4000, 5000 of 6000 switch door een van de volgende opdrachten uit te voeren:

- **set cam static**
- **set cam permanent**

Deze twee opdrachten hebben hetzelfde effect, behalve dat de statische items bij de herstart verdwijnen en de permanente items niet.

De tweede oplossing is om CGMP te gebruiken, wat een eigen Cisco-protocol is dat tussen de multicast router en de switch loopt. CGMP stelt de Cisco multicast router in staat om IGMP-berichten te begrijpen die door hosts worden verstuurd, en informeert de switch over de informatie in het IGMP-pakket.

De laatste (en meest efficiënte) oplossing is het gebruik van IGMP-snooping. Met IGMP snooping, onderbreekt de switch IGMP berichten van de gastheer zelf en werkt zijn MAC- tabel dienovereenkomstig bij. Geavanceerde hardware is vereist om IGMP-snooping te ondersteunen.

De CGMP-configuraties die in dit document worden gegeven, zijn voor Catalyst 4000 en 5000 switches met CatOS (CGMP wordt niet ondersteund op Catalyst 6000 switches) en IGMP-snoopingconfiguraties zijn voor Catalyst 5000 en 6000 switches met CatOS.

In de volgende sectie wordt een multicast adres kort beschreven, wordt de functionaliteit van IGMP uitgelegd en wordt extra informatie gegeven over CGMP en IGMP-snooping.

Multicastadres

1. Multicast IP-adressen zijn Klasse D IP-adressen. Daarom zijn alle IP-adressen van 224.0.0.0 tot 239.255.255.255 multicast IP-adressen. Zij worden ook aangeduid als GDA.
2. Voor elke GDA is er een gekoppeld MAC-adres. Dit MAC-adres wordt gevormd door 01-00-5e, gevolgd door de laatste 23 bits van de GDA, vertaald in hex, zoals hieronder wordt getoond.239.20.20.20 komt overeen met MAC 01-00-5e-14-14-14.239.10.10.10 komt overeen met MAC 01-00-5e-0a-0a-0a.Als gevolg daarvan is dit geen mapping van één naar één, maar een mapping van één naar veel. Van deze twee adressen, kunt u zien dat het eerste octet (239) niet in het adres van MAC wordt gebruikt. Dus de multicast adressen met dezelfde laatste drie octet maar de verschillende eerste octet hebben overlappende MAC adressen.
3. Sommige multicast IP-adressen zijn gereserveerd voor speciaal gebruik, zoals hieronder wordt getoond.224.0.0.1 - Alle multicast-geschikte hosts.224.0.0.2 - alle multicast-kabelrouters.224.0.0.5 en 224.0.0.6 worden gebruikt door Open Snelste pad (OSPF).

In het algemeen, worden de adressen van 224.0.0.1 tot 224.0.255 gereserveerd en gebruikt door verscheidene protocollen (standaard of eigen, zoals het protocol van de Hot Standby Router (HSRP)). Cisco raadt u aan deze niet voor GDA in een multicast netwerk te gebruiken. CGMP- en IGMP-snooping werken niet met dit gereserveerde adresbereik.

Internet Group Management-protocol

IGMP is een standaard die in RFC112 is gedefinieerd voor IGMPv1, in RFC2236 voor IGMPv2 en in RFC3376 voor IGMPv3. IGMP specificeert hoe een host zich met een router kan registreren om specifiek multicast verkeer te ontvangen. De volgende sectie geeft een kort overzicht van IGMP.

IGMPv1

IGMP versie 1 (IGMPv1)-berichten worden verzonden in IP-datagrammen en bevatten de volgende velden:

- Versie: 1
- Type: Er zijn twee soorten IGMP-berichten, Membership Search Query and Membership Report.
- checksum
- GDA

De lidmaatschapsrapporten worden uitgegeven door hosts die een specifieke multicast groep (GDA) willen ontvangen. De vragen van het lidmaatschap worden met regelmatige tussenpozen door routers verstrekt om te controleren of er nog een host in het GDA-segment is geïnteresseerd.

De rapporten van het gastlidmaatschap worden ofwel ongevraagd (wanneer de gastheer eerst het GDA-verkeer wil ontvangen) of in antwoord op een lidmaatschapsvraag verstrekt. Ze worden verzonden met de volgende velden:

L2-informatie

- Bron MAC: Host MAC-adres
- Bestemming MAC: BestemmingsMAC voor de GDA

L3-informatie

- Bron IP: IP-adres van de host
- Bestemming IP: GDA

IGMP-pakket

- De IGMP-gegevens bevatten bovendien de GDA en enkele andere gebieden.

De vragen van het lidmaatschap van de gastheer worden door de router naar het all-multicast adres verzonden: 224.0.0.1. Deze vragen gebruiken 0.0.0.0 in het IGMP GDA veld. Een host voor elke groep moet op die query reageren of de router stopt met het verzenden van het verkeer voor dat GDA naar dat segment (na drie pogingen). De router houdt een multicast routingstoegang voor elke bron bij en koppelt het aan een lijst van uitgaande interfaces (interface van waar het IGMP-rapport kwam). Na drie IGMP-query-pogingen zonder antwoord wordt deze interface gewist uit de vertrekkende interfacelijst voor alle items die gekoppeld zijn aan die GDA.

> **Opmerking:** IGMPv1 heeft geen verlofmechanisme. Als een gastheer het verkeer niet meer wil ontvangen, stopt het gewoon. Als het de laatste host op het net is, ontvangt de router geen antwoord op zijn query en verwijdert de GDA voor dat subtype.

IGMPv2

In IGMP versie 2 (IGMPv2) is het versieveld verwijderd en kan het typeveld nu verschillende waarden accepteren. De typen worden hieronder weergegeven.

- Membership Query
- IGMPv1-lidmaatschapsrapport
- Versie 2 Memberatierapport
- Verpakkingsgroep

Hieronder staan de beschrijvingen van de belangrijkste nieuwe functies die in IGMPv2 zijn toegevoegd.

- IGMP verlaat bericht: wanneer een host een groep wil verlaten, moet hij een IGMP-bericht van de Verlof naar bestemming 224.0.0.2 sturen (in plaats van in stilte te te vertrekken zoals in IGMPv1).
- Een router kan nu een groep-specifieke query verzenden door een Membership Query naar de groep GDA te verzenden in plaats van deze naar 0.0.0.0.

IGMPv3

In IGMP versie 3 (ICMPv3) is er een typeveld dat de volgende waarden kan hebben:

- Membership-vraag
- Versie 3 Memberatierapport

Een implementatie van IGMPv3 *moet* ook de volgende drie berichttypes ondersteunen, voor samenwerking met eerdere versies van IGMP:

- Versie 1 Membership Report [RFC112]

- Versie 2 Membership Report [RFC2236]
- Versie 2 Verlof Groep [RFC2236]

IGMPv3 voegt ondersteuning voor bronfiltering toe, dat wil zeggen de mogelijkheid voor een systeem om belang te melden bij het ontvangen van pakketten van specifieke bronadressen of van **alle maar** specifieke bronadressen die naar een specifiek multicast adres worden verzonden. Deze optie wordt ook Source Specific Multicast (SSM) genoemd.

Om een computer SSM te kunnen ondersteunen moet deze IGMPv3 ondersteunen. relatief weinig OS ondersteunen echter IGMPv3. Windows XP ondersteunt IGMPv3 en er zijn IGMPv3-ondersteuningspatches beschikbaar voor FreeBSD en Linux.

Beheerders moeten onderscheid maken tussen IGMPv3-ondersteuning op routerniveau en IGMPv3-snooping op het niveau van de switch. Het zijn twee verschillende kenmerken.

Ondersteuning van IGMPv3 op Catalyst Switches (L2)

- Catalyst 6000 met hybride mode-software (CatOS op Supervisor en Cisco IOS® Software op MSFC) ondersteunt officieel IGMPv3 snooping vanaf versie 7.5(1).
- In versies eerder dan 7.5(1) had de Catalyst 6000 switch geen officiële ondersteuning voor IGMPv3, maar deze zou normaal gesproken IGMPv3-pakketten moeten kunnen verwerken.
- Catalyst 6000 actieve geïntegreerde IOS-software ondersteunt IGMPv3 op routerniveau (L3-interface) vanaf versie 12.1(8a)E.
- Catalyst 4000 ondersteunt IGMPv3 alleen op routerniveau op supervisor III en IV. IGMPv3-snooping wordt niet ondersteund.

Ondersteuning van IGMPv3 op Cisco-routers (L3)

IGMPv3 wordt ondersteund op alle platforms die Cisco IOS® softwarerelease 12.1(5)T en latere releases gebruiken.

Caveats

Wanneer een switch IGMP snooping in werking stelt, onderbreekt het de pakketten IGMP en bevolkt de statische Layer 2 (L2) die tabel gebaseerd op de inhoud van de onderschept pakketten door te sturen. Wanneer er IGMPv1 of v2 hosts op het netwerk zijn, leest de switch de IGMP-toetredingen en -bladeren om te bepalen welke hosts welke multicast-stream wilt ontvangen, of te stoppen met het ontvangen van de multicast-stream.

IGMPv3 is gecompliceerder, omdat het niet alleen het groepsadres (multicast adres) gebruikt, maar ook de bronnen waarvan verkeer wordt verwacht. Naast de Catalyst 6000 switch die CatOS 7.5 of later en Native IOS versie 12.1(8a)E of later draait, zijn er momenteel geen andere switches die pakketten effectief kunnen sneeuwen en een verzendingstabel bouwen op basis van deze informatie. Daarom moet IGMP-snooping worden uitgeschakeld als er een IGMPv3-host op de switch staat. Wanneer IGMP-snooping is uitgeschakeld, kan de switch niet dynamisch een L2-verzendtabel maken voor de multicast-stromen. Met andere woorden: de switch overspoelt de multicast stromen.

Wanneer IGMP-snooping wordt uitgeschakeld, is één oplossing om multicast dynamische Content-Adresseerbare Geheugen (CAM)-items handmatig te configureren om overstroming van het subsysteem met multicast verkeer te voorkomen. Dit is echter een administratieve last en

geen dynamische oplossing. Wanneer een client het verkeer niet meer wil ontvangen, wordt de CAM-ingang niet uit de switch verwijderd (tenzij door handmatige handelingen), zodat het netwerkverkeer nog steeds aan de host is gericht.

Wanneer IGMPv3 in het netwerk wordt gebruikt, werken switches die CGMP gebruiken gewoonlijk anders dan het feit dat CGMP Fastleaving niet werkt. Als CGMP Fastleaving nodig is, is het het beste om terug te keren naar IGMPv2.

De openstaande platform-specifieke voorbehouden zijn te vinden in de release notes voor de respectieve switches.

Interoperabiliteit tussen IGMPv1 en IGMPv2

Met IGMPv1 en IGMPv2, stuurt slechts één router per IP SUBNET vragen. Deze router wordt de query router genoemd. In IGMPv1 wordt de query router geselecteerd met de hulp van het multicast routingprotocol. In IGMPv2 wordt het gekozen door het laagste IP-adres onder de routers. Hieronder staan verschillende mogelijkheden:

Scenario 1: IGMPv1-router met een mix van IGMPv1- en IGMPv2-hosts

De router begrijpt het IGMPv2 rapport niet, en daarom moeten alle hosts alleen het IGMPv1 rapport gebruiken.

Scenario 2: IGMPv2-router met een mix van IGMPv2- en IGMPv3-hosts

IGMPv1-hosts begrijpen de IGMPv2-query of de IGMPv2-groepslidmaatschapsvraag niet. De router moet IGMPv1 alleen gebruiken en de functie Verlader opschorten.

Scenario 3: IGMPv1 router en IGMPv2 op dezelfde segmentering geplaatst

De IGMPv1-router kan de IGMPv2-router niet detecteren. Daarom moet de IGMPv2-router door de beheerder als een IGMPv1-router worden geconfigureerd. Hoe dan ook, het kan zijn dat ze het niet eens zijn over de query router.

Interoperabiliteit tussen IGMPv1/IGMPv2 en IGMPv3

Met alle versies van IGMP, stuurt slechts één router per IP SUBNET vragen. Deze router wordt de query router genoemd. In IGMPv1 wordt de query router geselecteerd met de hulp van het multicast routingprotocol. In IGMPv2 en IGMPv3 wordt het gekozen door het laagste IP adres onder de routers. Hieronder staan verschillende interoperabiliteitsopties.

Scenario 1: IGMPv1/IGMPv2-router met een mix van IGMPv1/IGMPv2- en IGMPv3-hosts

Omdat de router de IGMPv3 rapporten niet begrijpt, gebruiken alle hosts de IGMPv1/IGMPv2 rapporten.

Scenario 2: IGMPv3-router met een mix van IGMPv1/IGMPv2- en IGMPv3-hosts

De IGMPv1/IGMPv2-hosts begrijpen de IGMPv3-query of IGMPv3-lidmaatschapsvraag niet. De

router moet alleen de IGMP versie gebruiken die overeenkomt met de laagste IGMP client versie die aanwezig is. Als er klanten IGMPv3 en IGMPv2 zijn, gebruikt de router IGMPv2. Als er klanten IGMPv1, IGMPv2 en IGMPv3 zijn, gebruikt de router IGMPv1.

Scenario 3: Andere versies van routers op hetzelfde segment

Wanneer routers van verschillende versies op hetzelfde segment aanwezig zijn, hebben de lager-versie routers geen middelen om de routers met hogere versies te detecteren. Daarom moeten de verschillende routers door de beheerder als dezelfde versie worden geconfigureerd. Deze versie moet overeenkomen met de laagste versie van een andere sprekende router die aanwezig is.

IGMP op een router

Als, door gebrek, is er geen gebruiker geregistreerd aan een specifieke groep in een netto, de router multicast verkeer voor die groep in die subnet niet doorstuurt. Dat betekent dat een router een IGMP rapport voor een GDA moet ontvangen om het aan de multicast routingtabel toe te voegen en verkeer voor die groep te beginnen verzenden.

Op een router moet u de volgende handelingen uitvoeren:

1. Schakel de multicast routing in de mondiale modus in, zoals hieronder wordt weergegeven.

   ```
   ip multicast-routing
   ```

2. Configureer een multicast routingprotocol op de betrokken interface, zoals hieronder wordt weergegeven.

   ```
   ip pim dense-mode
   ```

3. Controleer IGMP, zoals hieronder wordt getoond.

   ```
   show ip igmp interface
   show ip igmp group
   show ip mroute
   ```

4. Configureer een router om het IGMP-rapport (op de interface) te verzenden, zoals hieronder wordt weergegeven.

   ```
   ip igmp join-group [GDA_ip_address]
   ip igmp version [1 | 2 | 3]
   ```

Praktisch voorbeeld op een router

Een router wordt ingesteld op route tussen twee subinterfaces, Fast-Ethernet 0.2 en Fast-Ethernet 0.3. Beide interfaces zijn ook geconfigureerd om IGMP te gebruiken. In de onderstaande output kunt u de IGMP versie zien, de groep heeft zich aangesloten, enzovoort.

Configuratie

```
ip multicast-routing


interface FastEthernet0
 no ip address
 no ip directed-broadcast
!
interface FastEthernet0.2
 encapsulation isl 2
 ip address 10.2.2.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip pim dense-mode
!
interface FastEthernet0.3
 encapsulation isl 3
 ip address 10.3.3.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip pim dense-mode
!
```

show ip igmp interface

```
 Fa0.2 is up, line protocol is up
 Internet address is 10.2.2.1/24
 IGMP is enabled on interface
 Current IGMP version is 2
 CGMP is disabled on interface
 IGMP query interval is 60 seconds
 IGMP querier timeout is 120 seconds
 IGMP max query response time is 10 seconds
 Inbound IGMP access group is not set
 IGMP activity: 3 joins, 2 leaves
 Multicast routing is enabled on interface
 Multicast TTL threshold is 0
 Multicast designated router (DR) is 10.2.2.1 (this system)
 IGMP querying router is 10.2.2.1 (this system)
 Multicast groups joined: 224.0.1.40

 Fa0.3 is up, line protocol is up
 Internet address is 10.3.3.1/24
 IGMP is enabled on interface
 Current IGMP version is 2
 CGMP is disabled on interface
 IGMP query interval is 60 seconds
 IGMP querier timeout is 120 seconds
 IGMP max query response time is 10 seconds
 Inbound IGMP access group is not set
 IGMP activity: 1 joins, 1 leaves
 Multicast routing is enabled on interface
 Multicast TTL threshold is 0
 Multicast designated router (DR) is 10.3.3.1 (this system)
 IGMP querying router is 10.3.3.1 (this system)
 No multicast groups joined
```

show ip mroute and show ip igmp group

```
Router_A#show ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode


(*, 239.10.10.10), 00:01:15/00:02:59, RP 0.0.0.0, flags: DJC
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0.3, Forward/Dense, 00:01:16/00:00:00

(10.2.2.2, 239.10.10.10), 00:00:39/00:02:20, flags: CT
  Incoming interface: FastEthernet0.2, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0.3, Forward/Dense, 00:00:39/00:00:00

Router_A#show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
239.10.10.10     Fa0.3                00:02:48  00:02:04  10.3.3.2
Router_A#
```

Cisco-groepsbeheerprotocol

Raadpleeg voor CGMP-ondersteuning op Catalyst switches de Support Matrix van multicast Catalyst Switches.

CGMP-frames en Berichttypen

CGMP werd eerst geïmplementeerd door Cisco om multicast verkeer in een L2-netwerk te beperken. Omdat een switch in wezen niet naar L3-pakketten kan kijken, kan hij een IGMP-pakket niet onderscheiden. Met CGMP, verstrekt de router de interface tussen de hosts. De routers 'praten' IGMP en de switches 'praten' CGMP.

CGMP-frames zijn Ethernet-frames met het bestemmingadres 01-00-0c-dd-dd-dd en met een subnetwork Access Protocol (SNAP) header met de waarde 0x2001. De CGMP-frames bevatten de volgende velden:

- Versie: 1 of 2.
- Berichttype: Doe mee of ga weg.
- Grafiek: Het aantal multicast/unicast adresparen in het bericht.
- GDA: Het 48-bits MAC-adres van de multicast groep.
- Unicast Bron Adres (VS): Het 48-bits MAC unicast-adres van de apparaten die zich bij de GDA willen aansluiten.

  Opmerking: De waarde van het telveld bepaalt hoe vaak de laatste twee velden worden weergegeven.

Standaard luisteren de processors van een switch (NMP genoemd in Catalyst) alleen naar multicast adressen wanneer de **show cam system** commando wordt afgegeven. Wanneer u CGMP op een switch instelt, wordt het adres 01-00-0c-dd-dd-dd toegevoegd aan de **show cam system** opdrachtoutput.

De onderstaande tabel toont alle mogelijke CGMP-berichten.

GDA	Verenigde Staten	Samenvoegen/vertrekken	Betekenis
Mcast MAC	ClientMAC	Samenvoegen	Voeg poort toe aan groep.
Mcast MAC	ClientMAC	vertrekken	Verwijdert poort uit groep.
00-00-00-00-00-00	Router MAC	Samenvoegen	Pas routerpoort aan.
00-00-00-00-00-00	Router MAC	vertrekken	Kent routerpoort toe.
Mcast MAC	00-00-00-00-00-00	vertrekken	Vak verwijderen.
00-00-00-00-00-00	00-00-00-00-00-00	vertrekken	Alle groepen verwijderen.

Leerrouterpoorten

De switch moet zich bewust zijn van alle routerpoorten, zodat deze automatisch worden toegevoegd aan alle nieuwe multicast-items. De switch leert routerpoorten wanneer deze een CGMP-verbinding met GDA ontvangen 00-00-00-00-00-00 met Router MAC USA (derde type bericht in de tabel). Deze berichten worden door de router gegenereerd op alle interfaces die zijn geconfigureerd om CGMP te gebruiken. Er is echter ook een statische methode voor het configureren van routerpoorten op de switch.

Een groep aansluiten bij CGMP

- Een nieuwe klant vraagt om verkeer voor een GDA, dus de cliënt stuurt een IGMP rapport bericht.
- De router ontvangt het IGMP-rapport, verwerkt het en stuurt een CGMP-bericht naar de switch. De router kopieert het MAC-adres van de bestemming in het GDA-veld van de CGMP-aansluiting en kopieert het MAC-adres van de bron in de VS van de CGMP-aansluiting. Het stuurt het dan terug naar de switch.
- Een switch met CGMP-ondersteuning moet luisteren naar de CGMP-adressen met 01-00-0c-dd-dd-dd. De verwerker van de switch kijkt naar de CAM-tafel voor de VS. Zodra de VS in de CAM-tabel is opgenomen, weet de switch welke haven de VS aandoet.Maakt een nieuwe statische ingang voor de GDA en verbindt de haven van de VS met het hen samen met alle routerpoorten.Voeg de VS-haven toe aan de lijst van havens voor deze GDA (indien de statische vermelding al bestaat).

Een groep bij CGMP laten zitten

De statische ingangen die met CGMP worden geleerd zijn permanent, tenzij het overspannen van een verandering van de boomtopologie in VLAN plaatsvindt, of de router één van de laatste CGMP de berichten van het Verlof in de vorige tabel verstuurt.

Wanneer IGMPv1 de host is, stuurt u geen IGMP-verkenningsberichten. De router stuurt slechts berichten van het Verlof als het geen antwoord op drie opeenvolgende vragen van IGMP ontvangt. Dit betekent dat geen haven van een groep wordt verwijderd indien de gebruikers nog steeds geïnteresseerd zijn in die groep.

Met de introductie van IGMPv2 en de aanwezigheid van IGMP-verlof wordt Cisco toegevoegd aan de oorspronkelijke CGMP-specificatie (CGMPv2). Deze toevoeging wordt CGMP Fast-leaving genoemd.

Met CGMP Fast-leaving verwerking kan de switch IGMPv2 Verlof berichten naar het multicast-adres van de volledige router (224.0.0.2) door hosts op een van de poorten van de Supervisor Engine. Wanneer de module van de toezichthouder een bericht van het Verlor ontvangt, begint het een vraag-antwoord-timer en stuurt het een bericht naar de haven waarop dat verlof werd ontvangen om te bepalen of er nog een host is die deze multicast groep op die haven wil ontvangen. Als deze timer verloopt voordat een CGMP-opnambericht wordt ontvangen, wordt de poort vanaf de multicast-boom gesnoerd voor de multicast-groep die in het oorspronkelijke verlofbericht is gespecificeerd. Als het de laatste poort in de multicast groep is, verstuurt het bericht van het IGMP om te vertrekken naar alle routerpoorten. De router start dan het normale proces voor het wissen door een groep-specifieke query te verzenden. Omdat geen reacties worden ontvangen, verwijdert de router deze groep uit de multicast routingtabel voor die interface. Het stuurt ook een CGMP Verlaat bericht naar de switch die de groep uit de statische tabel verwijdert. Snelle verlaat verwerking waarborgt optimaal bandbreedtebeheer voor alle hosts op een geschakeld netwerk, zelfs wanneer meerdere multicast groepen tegelijkertijd in gebruik zijn.

Als het CGMP-verlof is ingeschakeld, worden twee items toegevoegd aan **show cam system** opdrachtoutput, zoals hieronder wordt getoond.

```
01-00-5e-00-00-01
01-00-5e-00-00-02
```

IGMP Verlof gebruikt 224.0.0.2 en IGMP Query gebruikt 224.0.0.1.

Gebruik de volgende stappen om CGMP te problemen oplossen:

1. Vanwege een conflict met de HSRP wordt de verwerking van het CGMP-verlof standaard uitgeschakeld. HSRP gebruikt MAC-adres 10-00-5e-00-02, dat hetzelfde is als IGMP Verlaat met IGMP versie 2. Met CGMP Fast-leaving gaan alle HSRP-pakketten naar de switch CPU. Omdat een HSRP-bericht geen IGMP-pakket is, genereert de switch alle dergelijke berichten en stuurt deze naar alle routerpoorten. Routers die `hsrp` ontvangen, `hallo` of `hsrp` verliezen connectiviteit. Probeer daarom bij het oplossen van HSRP-problemen de CGMP Fast-leaving uit te schakelen.Om de CGMP de verwerking te activeren, geeft u de **set cgmp leave enable** uit.
2. Als CGMP de verwerking van het verlaten is toegelaten, leert de Catalyst 5000 familiepoort switch routerpoorten door PIM-v1, HSRP en CGMP zelfgemaakte berichten. Wanneer de CGMP de verwerking van het verlaten wordt uitgeschakeld, leert de Catalyst 5000 familiepoort op de router door alleen CGMP-zelfJoin-berichten.

3. CGMP spuit multicast verkeer niet af voor een IP-multicast adres dat in het MAC-adresbereik van 10-00-5E-00-00-00 tot 1-00-5E-00-00-FF wordt aangegeven. De gereserveerde IP multicast adressen, in het bereik 224.0.0 tot 24.0.255, worden gebruikt om lokaal IP multicast verkeer in één enkele L3 hop door te sturen.

CGMP- en bronAll-Network

Een bronnetwerk is een segment met slechts een bron multicast en geen echte client. Daarom bestaat de kans dat er in dat segment geen IGMP-rapporten worden gegenereerd. CGMP moet echter nog steeds de overstroming van deze bron beperken (alleen voor routergebruik). Als een router multicast verkeer op één interface zonder IGMP-rapport detecteert, wordt het geïdentificeerd als een multicast source-only netwerk. De router genereert een gezamenlijk bericht van CGMP voor zichzelf en de switch voegt deze groep eenvoudigweg toe (met alleen de routerpoort).

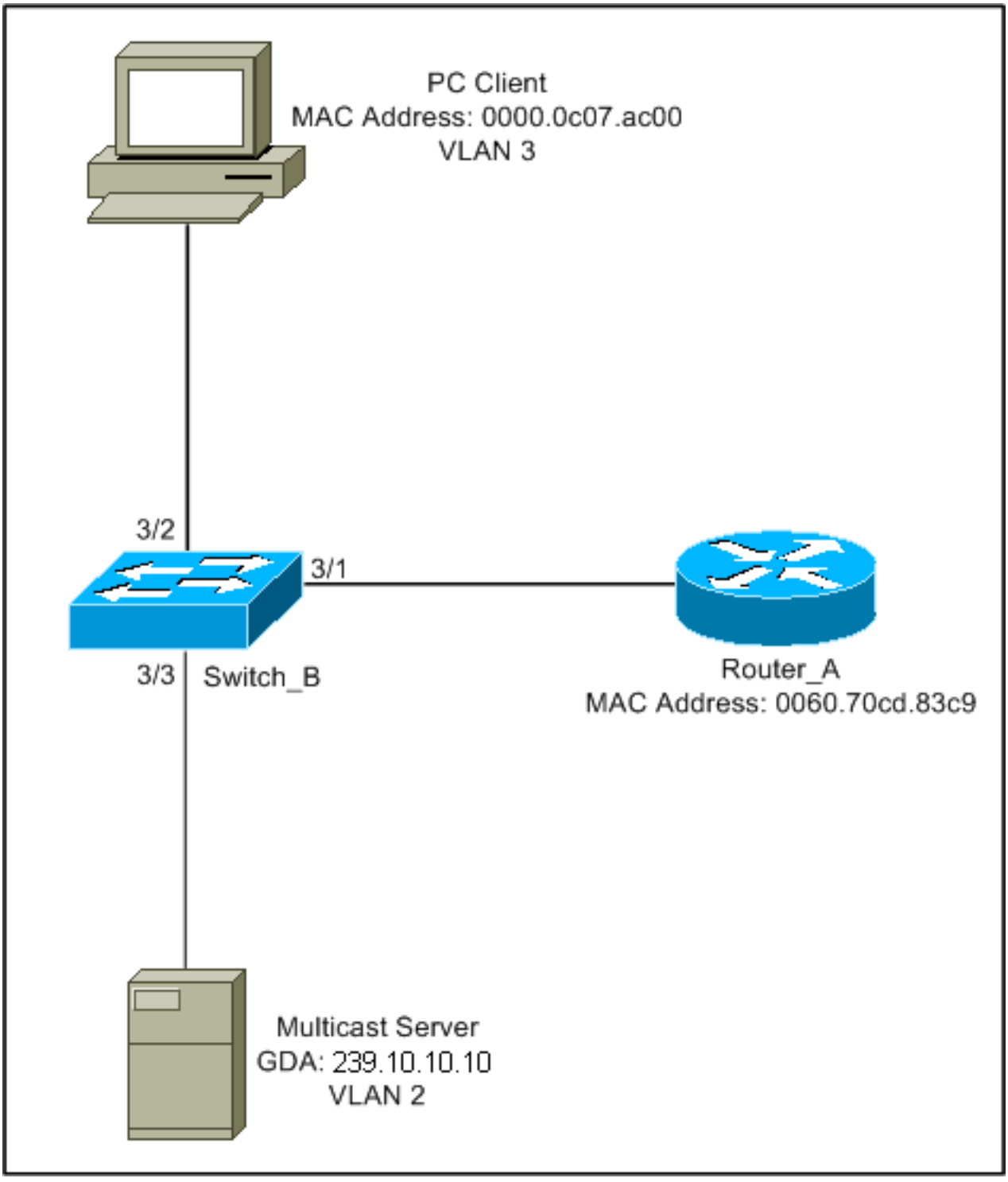
Cisco-routers en -Switches configureren om CGMP in te schakelen

De onderstaande opdrachten zijn alleen geldig voor Catalyst 4000- en 5000-serie (plus 2901, 2902, 2926, 2948G en 4912).

- MulticastrouterIP multicasting inschakelen (globale opdracht):**ip multicast-routing**Schakel elke interface met CGMP (interfacemodus) in met de volgende opdrachten:**ip pimip igmpip cgmp**Beken het L2 multicast probleem met de volgende opdrachten:**debug ip igmpdebug ip cgmp**
- Catalyst 4000 of 5000 Series-switchesCGMP inschakelen/uitschakelen met de volgende opdrachten:**set cgmp**CGMP Fast-leaving in- of uitschakelen met de volgende opdrachten:**set cgmp leave**Configureer de multicast router (statisch) met de volgende opdrachten:**set multicast router**Schakel de multicast router uit met de volgende opdrachten:**clear multicast router**Hieronder staan verschillende opdrachten om de CGMP-werking te controleren.**show cam staticshow cgmp statisticshow cgmp leaveshow multicast routershow multicast groupshow multicast group cgmpshow multicast group count**

Praktisch voorbeeld van CGMP van het gebruik en van Debug van opdracht en uitvoer

Dit is een praktisch configuratievoorbeeld voor een router van Cisco en een switch van de Catalyst.



Deze configuratie toont de operaties die betrokken zijn als een host zich bij een groep aansluit. Deze configuratie toont ook de bewerkingen omdat een host de groep verlaat met Fast-leaving. Er worden ook splintersporen en de configuratie van de switch en de router meegeleverd.

Een groep aansluiten bij CGMP

Raadpleeg deze stappen bij het aansluiten van een groep bij CGMP.

1. Schakel CGMP in op de switch, zoals hieronder wordt weergegeven.

```
Switch_B (enable) set cgmp en
MCAST-CGMP: Set CGMP Sys Entrie
MCAST-CGMP: Set CGMP Sys Entrie
MCAST-CGMP: Set CGMP Sys Entrie
```

```
CGMP support for IP multicast enabled.
Switch_B (enable)
```

Zoals u hieronder kunt zien, is vermelding 01-00-0c-dd-dd voor alle VLAN's in het menu **show cam system** opdrachtoutput. Bovendien, omdat het netwerk CGMP Fast-schapsverlof heeft, kunt u de items voor 01-00-5e-00-00-01 en 01-00-5e-00-02 zien.

```
Switch_B (enable) show cgmp leave

CGMP:       enabled
CGMP leave: enabled
Switch_B (enable) show cam system
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------ -----  -------------------------------------------
1     00-10-2f-00-14-00  #          7/1
1     00-e0-fe-4b-f3-ff  #          1/9
1     01-00-0c-cc-cc-cc  #          1/9
1     01-00-0c-cc-cc-cd  #          1/9
1     01-00-0c-dd-dd-dd  #          1/9
1     01-00-0c-ee-ee-ee  #          1/9
1     01-80-c2-00-00-00  #          1/9
1     01-80-c2-00-00-01  #          1/9
2     00-10-2f-00-14-00  #          7/1
2     01-00-0c-cc-cc-cc  #          1/9
2     01-00-0c-cc-cc-cd  #          1/9
2     01-00-0c-dd-dd-dd  #          1/9
2     01-80-c2-00-00-00  #          1/9
2     01-80-c2-00-00-01  #          1/9
3     01-00-0c-cc-cc-cc  #          1/9
3     01-00-0c-cc-cc-cd  #          1/9
3     01-00-0c-dd-dd-dd  #          1/9
3     01-80-c2-00-00-00  #          1/9
3     01-80-c2-00-00-01  #          1/9
Total Matching CAM Entries Displayed = 19
```

2. De router stuurt een gezamenlijk bericht van CGMP naar GDA 00-00-00-00-00-00 met de MAC van de router van de Verenigde Staten. Daarom wordt de routerpoort toegevoegd aan de lijst van de routerpoort (zie het eerste voorbeeld hieronder).**Op de router**

```
6d01h: CGMP: Sending self Join on Fa0.3
6d01h:       GDA 0000.0000.0000, USA 0060.70cd.83c9
```

Op de switch

```
MCAST-CGMP-JOIN: recvd CGMP JOIN msg on port 3/1 vlanNo 2
MCAST-CGMP-JOIN: join GDA 00-00-00-00-00-00 MCAST-CGMP-JOIN:USA
                 00-60-70-cd-83-c9
MCAST-ROUTER: Adding QUERIER port 3/1, vlanNo 2
MCAST-ROUTER: Creating RouterPortTimer for  port 3/1, vlanNo 2

Switch_B (enable) show multi router
CGMP enabled
IGMP disabled

Port       Vlan
---------  ----------------
 3/1       2-3

Total Number of Entries = 1
'*' - Configured
```

3. De PC op 3/1 stuurt IGMP een rapport met de GDA: 239.10.10.10 (zie kader 2 hieronder). Hieronder wordt de **show ip igmp group** opdrachtoutput op de router Router_A.Dit toont aan dat de router nu verkeer voor 24.10.10.10 naar fa0.3 doorstuurt. Dit is een gevolg van de ontvangst van het IGMP-rapport van 10.3.3.2, dat de client-PC is.

```
Router_A#show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
239.10.10.10     Fa0.3                00:02:48  00:02:04  10.3.3.2
Router_A#
```

4. De router ontvangt het rapport en stuurt een gezamenlijk bericht van CGMP samen met de volgende informatie:Bron MAC: MAC-adres van de routerDest MAC: 01-00-cc-dd-dd-ddInhoud: MAC-adres van de client-pc (VS): 00-00-0c-07-ac-00 MAC-adres van de multicast groep: 01-00-5e-0a-0a-0a (zie frame 3 hieronder)**Op de router**

```
6d01h: IGMP: Received v2 Report from 10.3.3.2 (Fa0.3) for 239.10.10.10
6d01h: CGMP: Received IGMP Report on Fa0.3
6d01h:       from 10.3.3.2 for 239.10.10.10
6d01h: CGMP: Sending Join on Fa0.3
```

5. De switch met 01-00-cc-dd-dd in de **show cam system** opdrachtoutput heeft CGMP ingeschakeld. De switch kan het pakket verwerken.De switch maakt een raadpleging in de dynamische CAM-tabel om te bepalen op welke poort het MAC-adres van de client-pc zich bevindt. Het adres bevindt zich op poort 3/2 en de switch maakt een statische vermelding in de CAM-tabel voor 01-00-5e-0a-0a aan poort 3/2. De switch voegt ook de routerpoort 3/1 toe aan de statische ingang voor die GDA.**Op de switch**

```
MCAST-CGMP-JOIN: recvd CGMP JOIN msg on port 3/1 vlanNo 3
MCAST-CGMP-JOIN: join GDA 01-00-5e-0a-0a-0a MCAST-CGMP-JOIN:USA 00-60-5c-f4-bd-e2
MCAST-CGMP-JOIN: 3/2/3: index 81
MCAST-CGMP-JOIN: recvd CGMP JOIN msg on port 3/1 vlanNo 2
MCAST-CGMP-JOIN: join GDA 01-00-5e-00-01-28 MCAST-CGMP-JOIN:USA 00-60-70-cd-83-c9
MCAST-CGMP-JOIN: 3/1/2: index 80
```

6. Alle daaropvolgende verkeer voor multicast groep 239.10.10.10 wordt alleen naar deze poort in dit VLAN doorgestuurd. Hieronder staat de statische ingang in de Catalyst switch waar 3/1 de routerpoort is en 3/2 de clientpoort.

```
Switch_B (enable) show cam static
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  ------------------------------------------
3     01-00-5e-0a-0a-0a             3/1-2
Total Matching CAM Entries Displayed = 3
Switch_B (enable)
```

Een groep verlaten met CGMP Fast-schapsverlof

Het voorbeeld hieronder vereist dat de klant een IGMP versie 2 client is en dat Fast-leaving op de switch is ingeschakeld.

1. De volgende procedure maakt het mogelijk om CGMP snel te laten vertrekken. Kijk naar het

show cgmp leave opdrachtoutput om te bepalen of deze is ingeschakeld. Kijk ook naar het **show cam system** opdrachtoutput om te bepalen of de switch luistert naar 01-00-5e-00-00-01 en 01-00-5e-00-00-02 (adressen gebruikt voor het verlof).

```
Switch_B (enable) show cgmp leave

CGMP:       enabled
CGMP leave: enabled
Switch_B (enable) show cam sys
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  -------------------------------------------
1     00-10-2f-00-14-00  #          7/1
1     00-e0-fe-4b-f3-ff  #          1/9
1     01-00-0c-cc-cc-cc  #          1/9
1     01-00-0c-cc-cc-cd  #          1/9
1     01-00-0c-dd-dd-dd  #          1/9
1     01-00-0c-ee-ee-ee  #          1/9
1     01-80-c2-00-00-00  #          1/9
1     01-80-c2-00-00-01  #          1/9
2     00-10-2f-00-14-00  #          7/1
2     01-00-0c-cc-cc-cc  #          1/9
2     01-00-0c-cc-cc-cd  #          1/9
2     01-00-0c-dd-dd-dd  #          1/9
2     01-00-5e-00-00-01  #          1/9
2     01-00-5e-00-00-02  #          1/9
2     01-80-c2-00-00-00  #          1/9
2     01-80-c2-00-00-01  #          1/9
3     01-00-0c-cc-cc-cc  #          1/9
3     01-00-0c-cc-cc-cd  #          1/9
3     01-00-0c-dd-dd-dd  #          1/9
3     01-00-5e-00-00-01  #          1/9
3     01-00-5e-00-00-02  #          1/9
3     01-80-c2-00-00-00  #          1/9
Do you wish to continue y/n [n]?  y
Total Matching CAM Entries Displayed = 22
```

2. De cliënt stuurt een IMPG-bericht naar 224.0.0.2. De switch onderschept het en stuurt een IGMP Query naar de haven waarop hij het verlof ontvangt. Het volgende is: **debug** uitvoer in de switch:

```
MCAST-IGMP-LEAVE:Recvd leave on port 3/2 vlanNo 3
MCAST-IGMP-LEAVE:router_port_tbl[vlanNo].QueryTime = 0
MCAST-IGMP-LEAVE:deletion_timer = 1
MCAST-SEND:Transmitting IGMP Mac Based GS Query msg on port 3/2 vlanNo 3
MCAST-SEND:  Transmit Succeeded for IGMP Group Specific Query msg on port 3/2 vlanNo 3
```

3. Omdat geen respons werd ontvangen, stuurt de Catalyst het IGMP bericht naar de router toe, zoals hieronder wordt getoond.

```
MCAST-TIMER:IGMPLeaveTimer expired on port 3/2 vlanNo 3 GDA 01-00-5e-0a-0a-0a
MCAST-TIMER:IGMPLeaveTimer expiry: Transmit IGMP Leave on port 3/1 vlanNo 3
MCAST-SEND:Transmitting IGMP Leave msg on port 3/1 vlanNo 3
MCAST-SEND: Inband Transmit Succeeded for IGMP Leave Message on port 3/1 vlanNo 3
```

4. De router ontvangt een IGMP Verlof bericht, zodat het een CGMP Verlof bericht aan de switch verstuurt en de groep ook van zijn IGMP groeplijst verwijdert. Hieronder staat het

debug opdrachtoutput op de router.**Op de router**

```
IGMP: Received Leave from 10.200.8.108 (Fa0.3) for 239.10.10.10
IGMP: Send v2 Query on Fa0.3 to 239.10.10.10
IGMP: Send v2 Query on Fa0.3 to 239.10.10.10
CGMP: Sending Leave on Fa0.3
      GDA 0100.5e0a.0a0a, USA 0000.0000.0000
IGMP: Deleting 239.10.10.10 on Fa0.3
```

CGMP-Traces en -configuratie

Kader 1

Frame 1 is een gezamenlijk CGMP-frame voor GDA 00-00-00-00-00-00. Het wordt gebruikt om de routerpoort aan de lijst met routerpoorten toe te voegen.

```
ISL: ----- ISL Protocol Packet -----
     ISL:
     ISL: Destination Address              = 01000C0000
     ISL: Type                             = 0 (Ethernet)
     ISL: User                             = 0 (Normal)
     ISL: Source Address                   = 8C958B7B1000
     ISL: Length                           = 76
     ISL: Constant value                   = 0xAAAA03
     ISL: Vendor ID                        = 0x8C958B
     ISL: Virtual LAN ID (VLAN)            = 2
     ISL: Bridge Protocol Data Unit (BPDU) = 0
     ISL: Port Index                       = 193
     ISL: Reserved
     ISL:
ETHER: ----- Ethernet Header -----
     ETHER:
     ETHER: Destination = Multicast 01000CDDDDDD
!--- Send to the CGMP !--- macaddress present in show cam sys !--- command output.

     ETHER: Source      = Station Cisco11411E1
     ETHER: 802.3 length = 24
     ETHER:
LLC:  ----- LLC Header -----
     LLC:
     LLC:  DSAP Address = AA, DSAP IG Bit = 00 (Individual Address)
     LLC:  SSAP Address = AA, SSAP CR Bit = 00 (Command)
     LLC:  Unnumbered frame: UI
     LLC:
SNAP: ----- SNAP Header -----
     SNAP:
     SNAP: Vendor ID = Cisco1
     SNAP: Type = 2001 (CGMP)
     SNAP:
CGMP: ----- CGMP -----
     CGMP:
     CGMP: Version   = 16
     CGMP: Type      = 0 (Join)
     CGMP: Reserved
     CGMP: Count     = 1
     CGMP:
     CGMP: Group Destination Address and Unicast Source Address
     CGMP:
     CGMP:    GDA    =0000.0000.0000
```

```
     CGMP:    USA    =0000.0C14.11E1
!--- MAC address of the router. CGMP:
```

Het resultaat frame 1 is op de switch, waarbij 3/1 de poort is die op de router is aangesloten:

Frame 2

Frame 2 is een IGMP-lidmaatschapsrapport dat door de host wordt verzonden om te vragen (of te bevestigen) dat gebruikers verkeer voor groep 239.10.10.10 willen ontvangen.

```
ISL: ----- ISL Protocol Packet -----
     ISL:
     ISL: Destination Address              = 01000C0000
     ISL: Type                             = 0 (Ethernet)
     ISL: User                             = 0 (Normal)
     ISL: Source Address                   = 8C958B7B1000
     ISL: Length                           = 76
     ISL: Constant value                   = 0xAAAA03
     ISL: Vendor ID                        = 0x8C958B
     ISL: Virtual LAN ID (VLAN)            = 2
     ISL: Bridge Protocol Data Unit (BPDU) = 0
     ISL: Port Index                       = 195
     ISL: Reserved
     ISL:
ETHER: ----- Ethernet Header -----
     ETHER:
     ETHER: Destination = Multicast 01005E0A0A0A
!--- Destination is the GDA MAC. ETHER: Source = Station Cisco176DCCA !--- Sourced by the PC
connected in 3/1. ETHER: Ethertype = 0800 (IP) ETHER: IP: ----- IP Header ----- IP: IP: Version
= 4, header length = 20 bytes IP: Type of service = C0 IP: 110. .... = internetwork control IP:
...0 .... = normal delay IP: .... 0... = normal throughput IP: .... .0.. = normal reliability
IP: Total length = 28 bytes IP: Identification = 0 IP: Flags = 0X IP: .0.. .... = may fragment
IP: ..0. .... = last fragment IP: Fragment offset = 0 bytes IP: Time to live = 1 seconds/hops
IP: Protocol = 2 (IGMP) IP: Header checksum = CC09 (correct) IP: Source address = [10.1.1.2] IP:
Destination address = [224.10.10.10] IP: No options IP: IGMP: ----- IGMP header ----- IGMP:
IGMP: Version = 1 IGMP: Type = 6 (Ver2 Membership Report) IGMP: Unused = 0x00 IGMP: Checksum =
FFEA (correct) IGMP: Group Address = [224.10.10.10] IGMP:
```

Frame 3

Frame 3 is het CGMP-kader dat door de router naar de switch wordt gestuurd om de switch te vertellen om een statische ingang voor 10-00e-0a-0a toe te voegen.

```
ISL: ----- ISL Protocol Packet -----
     ISL:
     ISL: Destination Address              = 01000C0000
     ISL: Type                             = 0 (Ethernet)
     ISL: User                             = 0 (Normal)
     ISL: Source Address                   = 8C958B7B1000
     ISL: Length                           = 76
     ISL: Constant value                   = 0xAAAA03
     ISL: Vendor ID                        = 0x8C958B
     ISL: Virtual LAN ID (VLAN)            = 2
     ISL: Bridge Protocol Data Unit (BPDU) = 0
     ISL: Port Index                       = 193
     ISL: Reserved
     ISL:
ETHER: ----- Ethernet Header -----
     ETHER:
     ETHER: Destination = Multicast 01000CDDDDDD
     ETHER: Source      = Station Cisco11411E1
```

```
     ETHER: 802.3 length = 24
     ETHER:
LLC:  ----- LLC Header -----
     LLC:
     LLC:  DSAP Address = AA, DSAP IG Bit = 00 (Individual Address)
     LLC:  SSAP Address = AA, SSAP CR Bit = 00 (Command)
     LLC:  Unnumbered frame: UI
     LLC:
SNAP: ----- SNAP Header -----
     SNAP:
     SNAP: Vendor ID = Cisco1
     SNAP: Type = 2001 (CGMP)
     SNAP:
CGMP: ----- CGMP -----
     CGMP:
     CGMP: Version   = 16
     CGMP: Type      = 0 (Join)
     CGMP: Reserved
     CGMP: Count     = 1
     CGMP:
     CGMP: Group Destination Address and Unicast Source Address
     CGMP:
     CGMP:    GDA    =0100.5E0A.0A0A
!--- GDA MAC added in show cam static !--- command output.

     CGMP:    USA    =0000.0C76.DCCA
!--- MAC of the PC in 3/1. CGMP:
```

Hieronder staat de configuratie van de router en de switch.

```
 Router_A (router) Configuration:

 Router_A#write terminal
 Building configuration...

 Current configuration:
 !
 version 12.0
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname Router_A
 !
 !
 ip subnet-zero
 ip multicast-routing
 ip dvmrp route-limit 20000


 interface FastEthernet0
  no ip address
  no ip directed-broadcast
 !
 interface FastEthernet0.1
  encapsulation isl 1
  ip address 10.1.1.1 255.255.255.0
  no ip redirects
  no ip directed-broadcast
 !
 interface FastEthernet0.2
  encapsulation isl 2
  ip address 10.2.2.1 255.255.255.0
```

```
 no ip redirects
 no ip directed-broadcast
 ip pim dense-mode
 ip cgmp
!
interface FastEthernet0.3
 encapsulation isl 3
 ip address 10.3.3.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip pim dense-mode
 ip cgmp
!
```

Switch_B configuration for CGMP:

```
#cgmp
set cgmp enable
set cgmp leave enable
!
```

CGMP statistics for VLAN 3:

```
Switch_B (enable) show cgmp sta 3
CGMP enabled

CGMP statistics for vlan 3:
valid rx pkts received           109
invalid rx pkts received         0
valid cgmp joins received        108
valid cgmp leaves received       1
valid igmp leaves received       1
valid igmp queries received      63
igmp gs queries transmitted      1
igmp leaves transmitted          1
failures to add GDA to EARL      0
topology notifications received  0
Switch_B (enable)
```

IGMP-signalering

IGMP-snooping is een andere functie waarmee u direct IGMP-frames kunt opnemen. Raadpleeg voor IGMP-ondersteuning bij Catalyst switches de Support Matrix voor multicast Catalyst Switches.

IGMP-softwareoverzicht

IGMP-snooping, zoals impliciet onder de naam, is een functie die de switch in staat stelt om op het IGMP-gesprek tussen hosts en routers "in" te luisteren. Wanneer een switch een IGMP rapport van een host voor een bepaalde multicast groep hoort, voegt de switch het havennummer van de host toe aan de GDA-lijst voor die groep. En, wanneer de switch een IGMP Verlof hoort, verwijdert het de poort van de gastheer uit de CAM tabel ingang.

De routerpoort leren

De switch luistert naar de volgende berichten om routerpoorten te detecteren met een IGMP-

snooping:

- IGMP Membership query sturen naar 01-00-5e-00-00-01
- PIMv1 hallo sturen naar 01-00-5e-00-00-02
- PIMv2 hallo sturen naar 01-00-5e-00-00-0d
- DVMRP-tests verzenden naar 01-00-5e-00-04
- MOSPF-bericht verzenden naar 01-00-5e-00-05 of 06

Door IGMP-snooping op een switch in te schakelen, worden alle bovenstaande MAC-items toegevoegd aan de **show cam system** opdrachtoutput van de snooping switch. Zodra een routerpoort wordt gedetecteerd, wordt deze toegevoegd aan de poortlijst van alle GDAs in dat VLAN.

Lid worden van een groep met IGMP Snooping

De volgende twee verbindende scenario's:

Scenario A: Host A is de eerste host om zich bij een groep in het segment aan te sluiten.

1. Host A verstuurt een ongevraagd IGMP-rapport.
2. De switch onderschept het IGMP Membership rapport dat door de host werd gestuurd die zich bij de groep wilde aansluiten.
3. De switch creëert een multicast ingang voor die groep en koppelt het aan de haven waar het het rapport heeft ontvangen en aan alle routerpoorten.
4. De switch stuurt het IGMP rapport naar alle routerpoorten. Dit is zodat de router ook het IGMP rapport ontvangt, en zijn multicast routing tabel dienovereenkomstig bijwerkt.

Scenario B: Host B is nu de tweede host om zich bij dezelfde groep aan te sluiten.

1. Host B stuurt een ongevraagd IGMP-rapport.
2. De switch onderschept het IGMP Membership rapport dat door de host wordt verstuurd die zich bij de groep wil aansluiten.
3. De switch stuurt het IGMP-rapport niet noodzakelijkerwijs naar alle routerpoorten. Eigenlijk stuurt de switch IGMP rapporten naar routerpoorten met behulp van proxy-rapportage, en stuurt slechts één rapport per groep binnen de 10s door.

   Opmerking: Om groepslidmaatschap te handhaven, stuurt de multicast router een IGMP-vraag elke 60 seconden. Deze query wordt door de switch tegengehouden en naar alle poorten op de switch doorgestuurd. Alle hosts die leden zijn van het groepsantwoord dat query. Maar gegeven het feit dat de switch het antwoordrapport ook tegenhoudt, ziet de andere host niet elk van de andere rapporten en dus sturen alle hosts een rapport (in plaats van één per groep). De switch gebruikt dan ook Proxy Reporting om slechts één rapport per groep te verzenden onder alle ontvangen reacties.

Stel dat Host A de groep wil verlaten, maar Host B wil de groep nog ontvangen.

- De switch neemt het IGMP Verlaat bericht van host A.
- De switch geeft een groep-specifieke IGMP Query uit voor de groep op die poort (en alleen op die poort).
- Als de switch geen rapport ontvangt, gooit hij deze haven van de ingang weg. Als het antwoord van die haven krijgt, doet het niets en neemt het het verlof weg.
- Host B is nog steeds geïnteresseerd in die switch. Dit zou niet de laatste niet-routerpoort in de

ingang zijn. Daarom stuurt de switch het bericht van vertrek niet door.

Ga ervan uit dat Host B de groep wil verlaten en Host B de laatste gebruiker is die geïnteresseerd is in deze groep.

- De switch neemt het IGMP Verlaat bericht van host A.
- De switch geeft een groep-specifieke IGMP Query uit voor die groep op die poort.
- Als de switch geen rapport ontvangt, gooit hij deze haven van de ingang weg.
- Dit is de laatste niet-routerpoort voor die GDA. De switch wordt naar alle routerpoorten verzonden (IGMP) en de ingang uit de tabel verwijderd.

IGMP/CGMP-interactie

In sommige netwerken kunt u door hardwarebeperkingen mogelijk niet IGMP-snooping op alle switches uitvoeren. In dit geval moet u CGMP op bepaalde switches in hetzelfde netwerk uitvoeren.

Dit is een speciaal geval. De switch die IGMP-snooping uitvoert, detecteert CGMP-berichten en detecteert dat sommige switches in het netwerk CGMP uitvoeren. Daarom wordt een speciale IGMP-CGMP-modus ingesteld en wordt de proxy-rapportage uitgeschakeld. Dit is absoluut noodzakelijk voor de juiste werking van CGMP, omdat routers het bron-MAC-adres van het IGMP-rapport gebruiken om een CGMP-verbinding te maken. Routers die CGMP uitvoeren, moeten alle IGMP-rapporten zien, dus de proxy-rapportage moet worden uitgeschakeld. Alle rapporten die naar de router worden verzonden, dienen alleen te zijn die strikt nodig zijn voor het IGMP-snooping.

Multicast voor resources

Als het segment slechts één multicast server (multicast bron) en geen client bevat, zou u kunnen eindigen met een situatie waar u geen IGMP pakketten in dat segment hebt, maar u hebt veel multicast verkeer. In dit geval stuurt de switch het verkeer van die groep naar iedereen in het segment. Gelukkig kan een switch die IGMP snooping runt deze multicast stromen detecteren en een multicast ingang voor die groep met slechts de routerpoort toevoegen. Deze items zijn intern gemarkeerd als `mcast_source_only` en worden elke 5 minuten verouderd, of wanneer de routerpoort verdwijnt. Merk op dat zelfs na deze veroudering het adres binnen een paar seconden beschikbaar is als het verkeer doorgaat. Binnen de releaseperiode kunnen tijdelijke overstromingen in het VLAN voorkomen. Gebruik de **set igmp flooding enable | disable** uit. Nadat de overstroming is uitgeschakeld, veroudert de switch niet de alleen-bron-items.

Beperkingen

Net als bij CGMP worden GDA's die zich in kaart brengen van een MAC dat binnen het bereik 01-00-5e-00-00-xx valt, nooit door IGMP-snooping gesnoeid.

Configuratie van IGMP-signalering op Cisco-Switches

Geef de volgende opdracht op om IGMP-snooping in/uit te schakelen:

- **set igmp**

Om de multicast router (statisch) te configureren geeft u de volgende opdracht uit:

- **set multicast router**
- **clear multicast router** ***port*** **|** ***all>***

Om IGMP-statistieken te controleren en te controleren geeft u de volgende opdrachten uit:

- **show igmp statistics**
- **show multicast router**

Praktisch voorbeeld van IGMP-signalering

De instelling voor dit voorbeeld komt overeen met de CGMP-test die eerder in dit document is gebruikt. Het enige verschil is dat poort 3/2 en 3/3 beide verbonden zijn met hetzelfde VLAN en beide client-geconfigureerd zijn om zich aan te sluiten bij groep 224.10.10.10.

Het volgende voorbeeld verklaart verschillende manipulaties, bekijkt wat de switch doet en onderzoekt de resulterende output. In het volgende voorbeeld is *Switch_B* een Catalyst 5500 die IGMP snooping runt en *Router_A* is de multicast router verbonden met poort 3/1.

1. IGMP-snooping op de switch inschakelen en het resultaat bekijken door de **debug** uit. Merk op dat elke set items is toegevoegd aan de **show cam sys** opdrachtoutput, waardoor de routerpoort kan worden gedetecteerd via PIM, MOSPF, enzovoort.

```
Switch_B (enable)  set igmp en

MCAST-IGMP: Set Sys Entries
MCAST-SYS-ENTRIES: Add system Entries in vlan 1
MCAST-IGMP: Set Sys Entries
MCAST-SYS-ENTRIES: Add system Entries in vlan 2
MCAST-IGMP: Set Sys Entries
MCAST-SYS-ENTRIES: Add system Entries in vlan 3

IGMP feature for IP multicast enabled

Switch_B (enable) show cam sys
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------ -----  -------------------------------------------
1     00-10-2f-00-14-00  #          7/1
1     00-e0-fe-4b-f3-ff  #          1/9
1     01-00-0c-cc-cc-cc  #          1/9
1     01-00-0c-cc-cc-cd  #          1/9
1     01-00-0c-dd-dd-dd  #          1/9
1     01-00-0c-ee-ee-ee  #          1/9
1     01-00-5e-00-00-01  #          1/9
1     01-00-5e-00-00-04  #          1/9
1     01-00-5e-00-00-05  #          1/9
1     01-00-5e-00-00-06  #          1/9
1     01-00-5e-00-00-0d  #          1/9
1     01-80-c2-00-00-00  #          1/9
1     01-80-c2-00-00-01  #          1/9
2     00-10-2f-00-14-00  #          7/1
2     01-00-0c-cc-cc-cc  #          1/9
2     01-00-0c-cc-cc-cd  #          1/9
2     01-00-0c-dd-dd-dd  #          1/9
2     01-00-5e-00-00-01  #          1/9
2     01-00-5e-00-00-04  #          1/9
2     01-00-5e-00-00-05  #          1/9
2     01-00-5e-00-00-06  #          1/9
2     01-00-5e-00-00-0d  #          1/9
```

2. De switch ontvangt een PIMv2 pakket van router Router_A en voegt de routerpoort toe.

```
MCAST-IGMPQ:recvd a PIM V2 packet of type HELLO on the port 3/1 vlanNo 2
MCAST-ROUTER: Adding port 3/1, vlanNo 2
MCAST-ROUTER: Creating RouterPortTimer for  port 3/1, vlanNo 2
MCAST-IGMPQ:recvd a PIM V2 packet of type HELLO on the port 3/1 vlanNo 3
MCAST-ROUTER: Adding port 3/1, vlanNo 3
MCAST-ROUTER: Creating RouterPortTimer for  port 3/1, vlanNo 3

Switch_B (enable) show multi router
CGMP disabled
IGMP enabled

Port       Vlan
---------  ----------------
 3/1       2-3

Total Number of Entries = 1
'*' - Configured
Switch_B (enable)
```

3. Sluit een nieuwe host in groep 224.10.10.10 (op poort 3/2). Deze gastheer stuurt een IGMP-lidmaatschapsrapport. Het rapport wordt ontvangen, ingesneden door de switch, de ingang wordt toegevoegd, en het IGMP rapport wordt doorgestuurd naar de router.Op Switch_B

```
MCAST-IGMPQ:recvd an IGMP V2 Report on the port 3/2 vlanNo 3
      GDA 224.10.10.10
MCAST-RELAY:Relaying packet on port 3/1 vlanNo 3
MCAST-SEND: Inband Transmit Succeeded for IGMP RELAY msg on port 3/1
      vlanNo 3

Switch_B (enable) show cam static
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des [CoS] Destination Ports or VCs / [Protocol Type]
----  ------------------ ----- -------------------------------------------
3     01-00-5e-0a-0a-0a         3/1-2
```

4. Voeg meer gebruiker in VLAN 3 op poort 3/3 toe, zoals hieronder getoond.

```
Switch_B (enable) show cam static

  * = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.

  X = Port Security Entry

  VLAN Dest MAC/Route Des [CoS] Destination Ports or VCs / [Protocol Type]
  ---- ------------------ ----- -------------------------------------------
  3    01-00-5e-0a-0a-0a         3/1-3
```

5. Verwijder haven 3/2. Port 3/2 verstuurt een IGMP-verlofbericht; de switch stuurt een IGMP-groepsspecifieke query terug op poort 3/2 en start een timer. Als de timer afloopt zonder een reactie te ontvangen, verwijdert hij de poort van de groep.

```
MCAST-IGMPQ:recvd an IGMP Leave on the port 3/2 vlanNo 3 GDA 224.10.10.10
MCAST-IGMPQ-LEAVE:router_port_tbl[vlanNo].QueryTime = 0
MCAST-DEL-TIMER: Deletion Timer Value set to Random Value  1
MCAST-SEND:Transmitting IGMP Mac Based GS Query msg on port 3/2 vlanNo 3
```

```
MCAST-SEND:  Transmit Succeeded for IGMP Group Specific Query msg on port 3/2 vlanNo 3
MCAST-TIMER:IGMPLeaveTimer expired on port 3/2 vlanNo 3 GDA 01-00-5e-0a-0a-0a
MCAST-TIMER:IGMPLeaveTimer:delete leave timer


Switch_B (enable) show cam static
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN Dest MAC/Route Des [CoS] Destination Ports or VCs / [Protocol Type]
---- ------------------ ----- -------------------------------------------
3    01-00-5e-0a-0a-0a         3/1,3/3
```

6. De host op poort 3/3 verlaat de groep en verstuurt een IGMP-bericht om te vertrekken. Het enige verschil met het vorige punt is dat het IGMP Verlof bericht uiteindelijk naar de routerpoort wordt doorgestuurd.

```
MCAST-IGMPQ:recvd an IGMP Leave on the port 3/3 vlanNo 3 GDA 224.10.10.10
MCAST-SEND:Transmitting IGMP Mac Based GS Query msg on port 3/3 vlanNo 3
MCAST-SEND:  Transmit Succeeded for IGMP Group Specific Query msg on
             port 3/3 vlanNo 3
MCAST-TIMER:IGMPLeaveTimer expired on port 3/3 vlanNo 3 GDA
             01-00-5e-0a-0a-0a
MCAST-TIMER:IGMPLeaveTimer expiry: Transmit IGMP Leave on port 3/1
             vlanNo 3
MCAST-SEND:Transmitting IGMP Leave msg on port 3/1 vlanNo 3
MCAST-SEND: Inband Transmit Succeeded for IGMP Leave Message on port 3/1
             vlanNo 3
MCAST-TIMER:IGMPLeaveTimer:delete leave timer
```

De subnetconfiguratie is nu terug in het begin, zijn staat in Stap 1. De multicast ingang is verdwenen uit het begin **show cam static** opdrachtoutput.

Om te eindigen, bekijk een voorbeeld van het **show igmp static** opdrachtoutput, zoals hieronder wordt getoond.

```
Switch_B (enable) show igmp stat 2
IGMP enabled

IGMP statistics for vlan 2:
Total valid pkts rcvd:          329
Total invalid pkts recvd        0
General Queries recvd           82
Group Specific Queries recvd    0
MAC-Based General Queries recvd 0
Leaves recvd                    0
Reports recvd                   82
Queries  Xmitted                0
GS Queries Xmitted              0
Reports Xmitted                 0
Leaves Xmitted                  0
Failures to add GDA to EARL     0
Topology Notifications rcvd     0

Switch_B (enable) show igmp stat 3
IGMP enabled

IGMP statistics for vlan 3:
```

```
Total valid pkts rcvd:           360
Total invalid pkts recvd         0
General Queries recvd            93
Group Specific Queries recvd     6
MAC-Based General Queries recvd  0
Leaves recvd                     11
Reports recvd                    64
Queries  Xmitted                 0
GS Queries Xmitted               14
Reports Xmitted                  0
Leaves Xmitted                   10
Failures to add GDA to EARL      0
Topology Notifications rcvd      1
Switch_B (enable)
```

Gerelateerde informatie

- Ondersteuning van multicast Catalyst Switches
- IP-multicast ondersteuningspagina
- Cisco-technologieondersteuning
- Cisco-productondersteuning
- Technische ondersteuning en documentatie – Cisco Systems